[A] TIIVISTELMÄ - SAMMANDRAG

SUOMI-FINLAND

(FI)

Patentti- ja rekisterihallitus
Patent- och registerstyrelsen

(11) (21) Patenttihakemus - Patentansökan 924092

(51) Kv.lk.5 - Int.cl.5

H 04K 1/06

(22) Hakemispäivä - Ansökningsdag 11.09.92

(24) Alkupäivä - Löpdag 11.09.92

(41) Tullut julkiseksi - Blivit offentlig 14.03.93

(32) (33) (31) Etuoikeus - Prioritet

13.09.91 US 759312 P

(71) Hakija - Sökande

1. **American Telephone & Telegraph Company**, 32 Avenue of the Americas, New York, N.Y. 10013-2412, USA, (US)

(72) Keksijä - Uppfinnare

1. **Reeds, James Alexander, III.**, 127 Southgate Road, New Providence, N.J. 07974, USA, (US)
2. **Treventi, Philip Andrew**, 15 Candlewood Drive, Murray Hill, N.J. 07974, USA, (US)

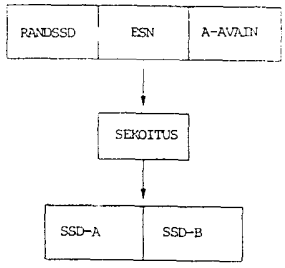
(74) Asiamies - Ombud: **Berggren Oy Ab**

(54) Keksinnön nimitys - Uppfinningens benämning

Puheen ja ohjaussanomien salakirjoittaminen solukkojärjestelmässä
Lönnskrift av tal och av styrningsmeddelanden i cellsystem

(57) Tiivistelmä - Sammandrag

Protokolla, joka todentaa asiakkaan matkaviestimen oikeaperäisyyden palvelun tuottajalle ja jossa signalointisanomat on salakirjoitettu ja jossa puheviestit voidaan salakirjoittaa. Palvelun tuottaja antaa jokaisen asiakkaan matkaviestimelle yksikäsitteisen "salaisuuden" sekä muuta informaatiota, kuten puhelinnumeron. Palvelun tuottajan niin halutessa asiakkaan matkaviestimelle lähetetään määräys, jonka mukaan se kehittää yhteisen salaisen tiedon tämän salaisuuden perusteella. Yhteinen salattu tieto kehitetään bittijonon avulla, jonka palvelun tuottaja tätä tarkoitusta varten lähettää. Osaa kehitetystä yhteisestä salaisesta tiedosta käytetään puheen salakirjoittamiseksi ja samaa tai muuta osaa kehitetystä yhteisestä salaisesta tiedosta käytetään syötteenä prosessille, joka kehittää toisen salakirjoitusavaimen. Tätä avainta käytetään asiakkaan matkaviestimessä niiden asiakkaan matkaviestimen kehittämien ohjaussignaalien koodaamiseksi, jotka vaikuttavat kulloinkin yhdistettynä olevan puhelun luonteeseen.



Jatkuu seur. sivulla
Forts. nästa sida

Protokoll som fastslår autenticiteten för en kunds mobila kommunikationsanläggning för servicetillställaren, och där signaleringsmeddelandena enkrypterats och där ljudkommunikationen kan enkrypteras. Servicetillställaren ger den mobila kommunikationsanläggningen för varje kund en entydig "hemlighet" samt övrig information, såsom ett telefonnummer. Om servicetillställaren så önskar sändes till kundens mobila kommunikationsanläggning en order enligt vilken den bildar en gemensam hemlig uppgift på basen av denna hemlighet. Den gemensamma hemliga uppgiften bildas medelst en bitlängd som servicetillställaren sänder för detta ändamål. En del av de bildade gemensamma hemliga uppgifterna användes för enkryptering av tal och samma del eller en annan del av de bildade gemensamma hemliga uppgifterna används för inmatning till en process som utvecklar en andra enkrypteringsnyckel. Denna nyckel används i kundens mobila kommunikationsanläggning för kodning av de styrsignaler som kundens mobila kommunikationsanläggning bildat vilka inverkar på naturen för samtalet som tillkopplats vid denna tidpunkt.